The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/10/2009

SUBJECT:
Vulnerabilities in Microsoft Windows Embedded OpenType Font Parsing Could allow for Remote Code Execution (MS09-065)

OVERVIEW:
A vulnerability has been discovered in the way Microsoft Windows parses Embedded OpenType Font (EOT) which could allow for remote code execution. Embedded OpenType Fonts are fonts within Microsoft Windows that are used for designing web pages and documents. These vulnerabilities can be exploited if a user opens a specially crafted file or webpage, including opening an e-mail attachment. Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:
Windows 2000
Windows XP
Windows 2003
Windows Vista
Windows 2008 (R2 Not Affected)

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft kernel-mode drivers that provide Embedded OpenType Font parsing that could allow remote code execution. These vulnerabilities can be exploited by opening a file, such as an email attachment, or through the Web. In the email based scenario, the user would have to open the specially crafted document or an HTML formatted email. In the Web based scenario, a user would visit a specially crafted web page.

The Embedded OpenType format is a special type of file designed to encapsulate one or more underlying fonts for distribution on a website. The fonts can be created using the Microsoft Web Embedding Fonts Tool (WEFT).

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.
- Read all e-mail messages in plain text.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-065.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2513
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2514

Security Focus:
http://www.securityfocus.com/bid/36029
http://www.securityfocus.com/bid/36939
http://www.securityfocus.com/bid/36941